Comprehensive Analysis of Image Encryption and Decryption Using J Component Methodology

1 Meet Raval, 2 Yogesh Pargai, 3Suraj Tiwari

ASM IMCOST

ABSTRACT:
Image encryption is an important aspect of protecting digital images from unauthorized access and ensuring confidentiality. A popular image encryption technique is the Arnold cat mapping technique, a chaos map-based approach that offers robust cryptographic properties. Arnold Cat's mapping technique is based on the concept of chaos theory and uses chaos maps to generate pseudorandom sequences that are highly sensitive to initial conditions. Arnold Cat maps are two-dimensional chaotic maps that manipulate images by rearranging pixels in a non-linear and deterministic way. The algorithm uses a permutation operation to periodically and repeatedly swap pixel positions, creating a chaotic pattern that spreads image pixels across the image. Arnold's cat mapping method offers several desirable properties for image encoding. First, because the encryption process is based on the chaotic behavior of the Arnold Cat card, it offers a high level of security as the encrypted image is resistant to attacks such as brute force and statistical analysis. Second, this technique offers excellent key confidentiality. A slight change in the encryption key produces a completely different encrypted image, ensuring confidentiality of the image data. Third, the technique has high cryptographic speed because permutation operations can be efficiently implemented using simple arithmetic operations.

Keywords: Arnold Cat Mapping, Chaotic Techniques, Cryptography, Encryption, Decryption.

INTRODUCTION:
Encryption is the process of transforming the original data, which is called plaintext, into encrypted data called ciphertext [1]. Different techniques are used to fulfill the data's own features of each data type. Many encryption algorithms are used to protect and encipher text data, such as the classical cipher system. Digital images are used in many communication applications, therefore the protection of the content of these images become very important. Image encryption is a technique which involves coding the original image (plain image) to another un-understanding image (cipher image). This technique must be provided by decoding the cipher image to plain image without losing data or image properties [3]. A diverse set of applications rely on digital image encryption and use various algorithms to protect the content and information of original images from unauthorized users. There are different types of encryption algorithms according to plaintext messages; some used for text data and not suitable for other multimedia data such as digital image. Other types used for images and not suitable for text data. Due to the powerful attributes of images, such as vast data capacity, great redundancy, and high correlation among pixels, encryption algorithms cannot be directly applied to images because of their large size. These algorithms require a significant amount of time when used with images. Another problem is that the decrypted text must be identical to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [4]. This paper presents textual encryption algorithms, such as the Vigenère and Hill cipher systems, which have been adapted and enhanced to encrypt and decrypt color digital images. The proposed system provides security to ensure that the original image can only be viewed or obtained by authorized individuals, integrity to guarantee that the image has not been altered, and confidentiality to ensure that the image remains secure during transmission. In this research, we use an algorithm which is used with raw data, and used in digital image Encryption and Decryption with some advances that are suitable with digital images. In this paper we try to overcome the limitations of AES and RSA in the encryption and decryption of digital images.
## LITERATURE SURVEY:

<table>
<thead>
<tr>
<th>Sr.no</th>
<th>Title &amp; author name</th>
<th>Methodology</th>
<th>Applications</th>
<th>Pros, Cons, Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Complex system structure</td>
</tr>
<tr>
<td>2.</td>
<td>M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A Modified AES Based Algorithm for Image Encryption</td>
<td>Modified AES Based Algorithm</td>
<td>Can be realizes both on hardware and software without any difficulties.</td>
<td>• W7 gives better encryption results in terms of security against statistical analysis attacks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• The key stream generator has an important influence on the encryption performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• overcome the problem of textured zones</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Offers flexibility allowing different key sizes</td>
</tr>
<tr>
<td>4.</td>
<td>Amador, Jose J., and Robert W. Green. “Symmetric-key block cipher for image and text cryptography.” International Journal of Imaging Systems and Technology 15.3 (2005): 178-188.</td>
<td>NASA/Kennedy Cipher (N/KC)</td>
<td>As it is a new cipher method its applications are yet to be defined.</td>
<td>• Empirical results are presented on N/KC’s ability of encrypting and decrypting text data in the form of vectors and documents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• management of the public-key and its storage is an on-going issue</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Davis, R. &quot;The data encryption standard in perspective.&quot; IEEE Communications Society Magazine 16.6 (1978): 5-9.</td>
<td>DES How the environment around des works and its various applications objectives of additional standards to be developed within the computer security program</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Highly sensitive to initial values and parameters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Complex system since key value is generated using henon map and pixel shuffling is done using Arnold cat map.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. This method can safeguard the image without reducing the value or information of a digital image that is secured</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Resists Brute force attacks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Small changes in original image and key leads to changes in the encrypted image and original cannot be accessed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Exploit explicit vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. resist against the differential attacks and robustness against different signal processing attacks and operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Vulnerability to brute force attacks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authors</td>
<td>Title</td>
<td>Techniques</td>
<td>Advantages</td>
</tr>
<tr>
<td>---</td>
<td>------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
- Robustness against image manipulation  
- Robustness against statistical attacks |
- Limited to black and white images  
- Time complexities need to be reduced |
- permutations and diffusions are performed several times in alternation to achieve a satisfactory security level. |
| 16| Khade, Pawan N., and Manish Narnaware | "3D chaotic functions for image encryption." International Journal of Computer Science Issues (IJCSI) 9.3 (2012): 323. | 3D chaotic algorithms and use of Chebyshev map to generate keys | - Provides higher key sensitivity  
- The system is more complex as it uses 3 additional keys  
- 3D Arnold's Cat map is used for additional scrambling and substitution |
| 17| Kankanpor, Jyoti TG, and Nitesh Naik | "Image security using image encryption and image stitching.” 2017 International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2017. | Image stitching | - Difficult for the attackers to steal the information conveyed through the user to the receiver |
- Confusion method is not secure enough |
EXISTING METHODS:

There are several existing methods for image encryption, some of which are:

1. **Substitution-permutation network (SPN) encryption:** This method involves using a combination of substitution and permutation operations to encrypt an image.
2. **Feistel network-based encryption:** This method is based on the use of Feistel networks, which involve splitting an image into two halves, and then encrypting each half using a key-dependent function.
3. **Chaos-based encryption:** This method involves using chaotic systems to generate the encryption key, which is then used to scramble the image.
4. **Public key-based encryption:** This method involves using a public key to encrypt an image, which can then only be decrypted using the corresponding private key.
5. **DNA-based encryption:** This method involves encoding an image using DNA sequences, which can then be decoded using DNA sequencing technology.
6. **Steganography-based encryption:** This method involves hiding an image within another image, so that it is not visible to the naked eye, and can only be accessed using a secret key.
7. **Quantum-based encryption:** This method involves using quantum cryptography principles to encrypt an image, which ensures high levels of security.

PROPOSED WORK:

For encryption:

1. Input the original image to be encrypted.
2. Define the encryption parameters, such as the number of iterations and the encryption key. Apply the Arnold Cat mapping algorithm to permute the pixels of the original image. The algorithm typically involves the following steps:
3. Calculate the new position of each pixel using the following formulas:
   \[
   \text{New}_X = (a \cdot X + b \cdot Y) \mod \text{Image\_Width} \\
   \text{New}_Y = (c \cdot X + d \cdot Y) \mod \text{Image\_Height}
   \]
where \( X \) and \( Y \) represent the original coordinates of the pixel, and \( a, b, c, d \) are the parameters of the Arnold Cat map obtained from the encryption key. Update the pixel values in the new positions to obtain the encrypted image.

4. Repeat the permutation process for the desired number of iterations.

5. Output the encrypted image.

For decryption:

1. Input the encrypted image to be decrypted.

2. Define the decryption parameters, such as the number of iterations and the decryption key (which should match the encryption key). Apply the inverse Arnold Cat mapping algorithm to reverse the permutation of the encrypted image. The algorithm typically involves the following steps:

   a. Calculate the original position of each pixel using the following formulas:

   \[
   \text{Old}_X = (d \times X - b \times Y) \mod \text{Image Width} \\
   \text{Old}_Y = (-c \times X + a \times Y) \mod \text{Image Height}
   \]

   where \( X \) and \( Y \) represent the encrypted coordinates of the pixel, and \( a, b, c, d \) are the parameters of the Arnold Cat map obtained from the decryption key. Update the pixel values in the original positions to obtain the decrypted image.

3. Repeat the inverse permutation process for the desired number of iterations.

4. Output the decrypted image.

REFERENCES: